



Handleiding Desktop Management

Zakelijke desktopcomputers

Artikelnummer van document: 312947-332

September 2003

Deze handleiding bevat definities en instructies voor het gebruik van de functies voor beveiliging en Intelligent Manageability (Client Management), die op bepaalde modellen vooraf zijn geïnstalleerd.

© 2003 Hewlett-Packard Development Company, L.P.

HP, Hewlett Packard en het Hewlett-Packard logo zijn handelsmerken van Hewlett-Packard Company in de Verenigde Staten en andere landen.

Compaq en het Compaq logo zijn handelsmerken van Hewlett-Packard Development Company, L.P. in de Verenigde Staten en andere landen.

Microsoft, MS-DOS, Windows en Windows NT zijn handelsmerken van Microsoft Corporation in de Verenigde Staten en andere landen.

Alle overige productnamen in deze publicatie kunnen handelsmerken zijn van hun respectievelijke houders.

Hewlett-Packard Company aanvaardt geen aansprakelijkheid voor technische fouten, drukfouten of weglatingen in deze publicatie. Ook aanvaardt Hewlett-Packard Company geen aansprakelijkheid voor incidentele schade of voor schade die wordt veroorzaakt door verstrekking, eventuele ondoelmatigheid of gebruik van dit materiaal. De informatie in deze handleiding wordt zonder garantie verstrekt, daaronder mede begrepen maar niet beperkt tot impliciete garanties betreffende verkoopbaarheid of geschiktheid voor een bepaalde toepassing, en kan zonder voorafgaande kennisgeving worden gewijzigd. De garanties op HP producten worden beschreven in de garantieverklaringen behorende bij deze producten. Niets in deze handleiding kan worden opgevat als een aanvullende garantie.

De informatie in dit document valt onder het auteursrecht. Dit document of een gedeelte hiervan mag niet worden gekopieerd, vermenigvuldigd of vertaald in een andere taal, zonder voorafgaande schriftelijke toestemming van Hewlett-Packard Company.



WAARSCHUWING: Als u de aanwijzingen na dit kopje niet opvolgt, kan dit leiden tot persoonlijk letsel of levensgevaar.



VOORZICHTIG: Als u de aanwijzingen na dit kopje niet opvolgt, kan dit beschadiging van de apparatuur of verlies van gegevens tot gevolg hebben.

Handleiding Desktop Management

Zakelijke desktopcomputers

Tweede editie (september 2003)

Artikelnummer van document: 312947-332

Inhoudsopgave

Handleiding Desktop Management

Eerste configuratie en ingebruikneming	2
Remote System Installation (Systeeminstallatie op afstand)	3
Software bijwerken en beheren	4
HP Client Manager	4
Altiris-oplossingen	4
Altiris PC Transplant Pro	5
System Software Manager (SSM)	6
Proactive Change Notification	6
ActiveUpdate	6
ROM-flash	7
Remote ROM Flash (ROM-flash op afstand)	7
HPQFlash	8
FailSafe Boot Block ROM (FailSafe ROM met opstartblok)	8
Computerinstellingen kopiëren	10
Aan/uit-knop met twee standen	18
Website	19
Bouwstenen en partners	20
Inventarisbeheer en beveiliging	20
Wachtwoordbeveiliging	25
Instelwachtwoord definiëren met Computer Setup (Computerinstellingen)	25
Opstartwachtwoord definiëren met Computer Setup (Computerinstellingen)	26
Embedded Security (Geïntegreerde beveiliging)	31
DriveLock	41
Smart Cover Sensor	43
Smart Cover Lock	44

MBR-beveiliging	46
Voordat u de huidige opstartschijf partitioneert of formateert	48
Kabelslotvoorziening	49
Identificatie van vingerafdrukken.....	49
Foutberichten en foutherstel	49
Schijfbeveiligingssysteem	50
Voedingseenheid met beveiliging tegen spanningspieken	50
Temperatuursensor	50

Index

Handleiding Desktop Management

HP Intelligent Manageability (Client Management) biedt op standaarden gebaseerde oplossingen voor het beheren en besturen van desktopcomputers, werkstations en notebookcomputers in een netwerkomgeving. HP heeft in 1995, met de introductie van de eerste desktopcomputers die volledig konden worden beheerd, het voortouw genomen op het gebied van desktopmanagement. HP is houder van een patent op technologie voor beheerssoftware. Sindsdien heeft de IT-sector onder leiding van HP gezamenlijke standaarden en infrastructuren ontwikkeld die vereist zijn om desktopcomputers, werkstations en notebookcomputers effectief te kunnen installeren, configureren en beheren. HP werkt nauw samen met toonaangevende leveranciers van beheerssoftware om de compatibiliteit tussen Intelligent Manageability (Client Management) en deze beheerapplicaties te waarborgen. Intelligent Manageability maakt een belangrijk onderdeel uit van onze inspanningen op velerlei gebied om u te voorzien van oplossingen voor de vier fasen van de levenscyclus van een desktopcomputer: planning, installatie, beheer en migratie.

De belangrijkste mogelijkheden en functies van Desktop Management zijn:

- eerste configuratie en ingebruikneming
- systeeminstallatie op afstand
- updates en beheer van software
- ROM-flash
- inventarisbeheer en beveiliging
- foutmeldingen en fouterstel



De ondersteuning voor specifieke functies die in deze handleiding worden beschreven, varieert per model of softwareversie.

Eerste configuratie en ingebruikneming

Uw computer wordt geleverd met een vooraf geïnstalleerd image van de systeemsoftware. Na een korte procedure waarin de software wordt “uitgepakt”, is de computer gereed voor gebruik.

Desgewenst kunt u het vooraf geïnstalleerde software-image vervangen door een aangepast pakket met systeem- en applicatiesoftware. Aangepaste software kan op verschillende manieren worden geïmplementeerd. Enkele manieren zijn:

- extra softwareapplicaties installeren nadat u het vooraf geïnstalleerde software-image heeft uitgepakt;
- gebruikmaken van systemen voor software-installatie, zoals Altiris Deployment Solution™, om de vooraf geïnstalleerde software te vervangen door een aangepast software-image;
- de inhoud van een vaste schijf naar een andere vaste schijf kopiëren via een kloonproces.

Welke voor u de beste installatiemethode is, hangt af van uw IT-omgeving en IT-processen. Het gedeelte PC Deployment op de website HP Lifecycle Solutions (<http://h18000.www1.hp.com/solutions/pcsolutions>) bevat informatie aan de hand waarvan u de beste installatiemethode kunt selecteren.

De cd *Restore Plus!*, de ROM-configuratie en de ACPI-hardware bieden hulp bij het herstellen van systeemsoftware, het beheer van de configuratie, probleemoplossing en bij energiebeheer.

Remote System Installation (Systeeminstallatie op afstand)

Met Remote System Installation (Systeeminstallatie op afstand) kunt u het systeem opstarten en instellen met behulp van de software en configuratiegegevens die op een netwerkserver aanwezig zijn. Hierbij maakt u gebruik van de Preboot Execution Environment (PXE). Deze voorziening wordt gewoonlijk gebruikt als hulpmiddel voor het instellen en configureren van een systeem en kan voor de volgende taken worden gebruikt:

- vaste schijf formatteren;
- software-image installeren op een of meer nieuwe pc's;
- systeem-BIOS in flash-ROM op afstand updaten ("[Remote ROM Flash \(ROM-flash op afstand\)](#)" op pagina 7);
- instellingen van het systeem-BIOS configureren.

U start Remote System Installation door op **F12** te drukken zodra het bericht F12 = Network Service Boot (Opstarten via netwerkservice) rechtsonder in het scherm met het HP logo verschijnt. Volg de instructies op het scherm om door te gaan. De standaard opstartvolgorde is een instelling van de BIOS-configuratie. Deze kunt u wijzigen om het systeem altijd te laten proberen op te starten met PXE.

HP en Altiris, Inc. hebben de krachten gebundeld om hulpprogramma's te maken die bedoeld zijn om de ingebruikneming en het beheer van bedrijfscomputers gemakkelijker en minder tijdrovend te maken. Hierdoor worden uiteindelijk de exploitatiekosten lager en zijn in een bedrijfsomgeving HP computers de best te beheren clientcomputers.

Software bijwerken en beheren

HP biedt verschillende hulpmiddelen voor het beheren en bijwerken van software op desktopcomputers en werkstations: Altiris, Altiris PC Transplant Pro, HP Client Manager Software (een Altiris-oplossing), System Software Manager, Proactive Change Notification en ActiveUpdate.

HP Client Manager

Intelligente HP Client Manager Software (HP CMS) biedt een nauwe integratie van HP Intelligent Manageability (Client Management) met Altiris, hetgeen leidt tot een uitstekende beheerfunctionaliteit voor HP apparaten. Enkele van de beschikbare functies zijn:

- gedetailleerde overzichten van de hardware-inventaris ten behoeve van het inventarisbeheer;
- controle en diagnostiek van de toestand van de computer;
- proactieve informatie over wijzigingen in de hardwareomgeving;
- meldingen via een webinterface over essentiële gebeurtenissen zoals computers met temperatuurwaarschuwingen, geheugenfouten en dergelijke;
- updates op afstand van systeemsoftware, zoals stuurprogramma's en ROM BIOS;
- op afstand wijzigen van de opstartvolgorde.

Ga voor meer informatie over HP Client Manager naar:
http://h18000.www1.hp.com/im/client_mgr.html.

Altiris-oplossingen

HP Client Management-oplossingen bieden gecentraliseerd hardwarebeheer van HP clientapparaten voor alle stadia van de IT-levenscyclus.

- inventarisbeheer
 - ❑ naleving van softwarelicenties
 - ❑ computerbewaking en rapportage
 - ❑ leasecontract, vastlegging van inventarisbeheer

- ingebruikneming en migratie
 - ☐ migratie van Microsoft Windows 2000 of Windows XP Professional of Home Edition
 - ☐ ingebruikneming van computersystemen
 - ☐ migratie van voorkeursinstellingen
- helpdesk en probleemoplossing
 - ☐ beheer van helpdeskmeldingen
 - ☐ op afstand problemen opsporen
 - ☐ op afstand problemen verhelpen
 - ☐ calamiteitenherstel voor clients
- softwarebeheer en operationeel beheer
 - ☐ doorlopend desktopbeheer
 - ☐ ingebruikneming van HP systeemsoftware
 - ☐ zelfherstel van applicaties

Op bepaalde desktop- en notebookmodellen maakt een Altiris Management Agent deel uit van het in de fabriek geïnstalleerde image. Deze agent maakt de communicatie mogelijk met de Altiris Development Solution, die kan worden gebruikt om met eenvoudigheid te voeren wizards nieuwe hardware in gebruik te nemen of voorkeursinstellingen te migreren naar een nieuw besturingssysteem. Altiris-oplossingen bieden eenvoudige functies voor software distributie. Wanneer u Altiris gebruikt in combinatie met System Software Manager of HP Client Manager, kunt u hiermee ook het ROM-BIOS en stuurprogramma's bijwerken vanaf een centrale console.

Ga voor meer informatie naar <http://www.hp.com/go/easydeploy>.

Altiris PC Transplant Pro

Altiris PC Transplant Pro maakt probleemloze computermigratie mogelijk door oude instellingen, voorkeuren en gegevens te bewaren en snel en eenvoudig te migreren naar de nieuwe omgeving. Een upgrade kost nog maar enkele minuten in plaats van uren of dagen, en het bureaublad heeft precies het uiterlijk en de functionaliteit die de gebruikers verwachten.

Bezoek de website

<http://h18000.www1.hp.com/im/prodinfo.html#deploy> voor meer informatie over het downloaden van een gedurende 30 dagen volledig functionele evaluatieversie.

System Software Manager (SSM)

System Software Manager (SSM) is een hulpprogramma waarmee u op meerdere computers tegelijk een update van de systeemsoftware kunt uitvoeren. Wanneer u SSM uitvoert op een clientcomputer, worden de versies van zowel de hardware als de software gedetecteerd, waarna de update van de software wordt uitgevoerd vanaf een centrale opslagplaats. Stuurprogramma's met SSM-ondersteuning worden op de stuurprogrammawebsite en op de cd met ondersteunende software aangegeven met een speciaal pictogram. Als u het hulpprogramma wilt downloaden of als u meer informatie wilt opvragen over SSM, bezoekt u <http://h18000.www1.hp.com/im/ssmwp.html>.

Proactive Change Notification

Het programma Proactive Change Notification maakt gebruik van de beveiligde website Subscriber's Choice om proactief en automatisch het volgende te verzorgen:

- U ontvangt per e-mail PCN-berichten (Proactive Change Notification) waarmee u tot 60 dagen van tevoren wordt ingelicht over hardware- en softwarewijzigingen in de meeste commercieel verkrijgbare computers en servers.
- U ontvangt e-mailberichten met Customer Bulletins, Customer Advisories, Customer Notes, Security Bulletins en Driver Alerts voor de meeste commercieel verkrijgbare computers en servers.

U definieert uw eigen profiel, zodat u alleen informatie ontvangt die betrekking heeft op een specifieke IT-omgeving. Als u meer wilt weten over het programma Proactive Change Notification en een eigen profiel wilt opstellen, gaat u naar <http://www.hp.com/go/pcn>.

ActiveUpdate

ActiveUpdate is een clientapplicatie van HP. De ActiveUpdate-client wordt op het lokale systeem uitgevoerd en maakt gebruik van een gebruikersprofiel om proactief en automatisch software-updates voor de meeste commerciële HP computers en servers te downloaden. Deze gedownloade software-updates kunnen met HP Client Manager en System Software Manager op intelligente wijze worden geïnstalleerd op de computers waarvoor ze zijn bedoeld.

Om meer informatie over ActiveUpdate te krijgen, om de applicatie te downloaden of om uw eigen profiel te maken, bezoekt u <http://h18000.www1.hp.com/products/servers/management/activeupdate/index.html>.

ROM-flash

De computer heeft een programmeerbaar flash-ROM (Read Only Memory). Door een instelwachtwoord te definiëren in Computer Setup (Computerinstellingen) kunt u voorkomen dat het ROM onbedoeld wordt gewijzigd of overschreven. Dit is belangrijk om de bedrijfszekerheid van de computer te waarborgen. Als u het ROM wilt upgraden, kunt u het volgende doen:

- Bestel een ROMPaq upgradedishette bij HP.
- Download de meest recente ROMPaq-images van de website <http://h18000.www1.hp.com/im/ssmwp.html>.



VOORZICHTIG: Zorg ervoor dat u een instelwachtwoord definieert om het ROM optimaal te beschermen. Het instelwachtwoord voorkomt ROM-upgrades door onbevoegden. Met behulp van System Software Manager kan de systeembeheerder het instelwachtwoord voor een of meer computers tegelijk definiëren. Voor meer informatie bezoekt u <http://h18000.www1.hp.com/im/ssmwp.html>.

Remote ROM Flash (ROM-flash op afstand)

Met een ROM-flash op afstand kan de systeembeheerder het ROM van HP computers op afstand veilig upgraden vanaf de centrale beheerdersconsole. Doordat de systeembeheerder deze taak op afstand uitvoert voor meerdere computers tegelijk, is een consistent gebruik van en betere controle op ROM-versies van HP computers in het gehele netwerk mogelijk. Bovendien leidt dit tot een hogere productiviteit en lagere onderhoudskosten.



De computer moet zijn ingeschakeld of op afstand worden geactiveerd om van de flash-ROM-upgrade te kunnen profiteren.

Voor meer informatie over ROM-flash op afstand raadpleegt u HP Client Manager Software of System Software Manager op de website <http://h18000.www1.hp.com/im/prodinfo.html>.

HPQFlash

Het hulpprogramma HPQFlash wordt gebruikt om het systeem-ROM op afzonderlijke computers lokaal te updaten of herstellen via een Windows-besturingssysteem.

Ga voor meer informatie over HPQFlash naar
<http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18607.html>.

FailSafe Boot Block ROM (FailSafe ROM met opstartblok)

Het FailSafe Boot Block ROM (FailSafe ROM met opstartblok) zorgt dat het systeem zich kan herstellen in het onwaarschijnlijke geval dat zich een storing voordoet bij het flashen van het ROM, bijvoorbeeld wanneer de stroom uitvalt tijdens een ROM-upgrade. Het opstartblok is een tegen flashen beveiligd gedeelte van het ROM dat bij het inschakelen van het systeem controleert of de systeem-ROM-flash geldig is.

- Als het systeem-ROM geldig is, start het systeem normaal.
- Als het systeem-ROM niet door de controle komt, biedt het FailSafe ROM met opstartblok voldoende ondersteuning om het systeem op te starten vanaf een ROMPaq diskette, waarmee het systeem-ROM van een geldige ROM-versie kan worden voorzien.

Als er een ongeldig systeem-ROM wordt gedetecteerd, knippert het aan/uit-lampje 8 maal in de kleur ROOD met tussenpozen van 1 seconde, gevolgd door een pauze van 2 seconden. Bovendien klinken er tegelijkertijd 8 geluidssignalen. Op het scherm verschijnt een bericht over het herstel van het ROM met behulp van het opstartblok (dit geldt alleen voor bepaalde modellen).


In de herstelstand kunt u het systeem als volgt herstellen:

1. Als er een diskette in de diskettedrive aanwezig is, verwijdt u de diskette en vervolgens schakelt u de computer uit.
2. Plaats een ROMPaq diskette in de diskettedrive.
3. Schakel de stroom voor het systeem weer in.
4. Als geen ROMPaq diskette wordt aangetroffen, wordt u gevraagd deze in de diskettedrive te plaatsen en de computer opnieuw op te starten.

5. Als een instelwachtwoord is gedefinieerd, gaat het Caps Lock-lampje branden en wordt u gevraagd het wachtwoord in te voeren.
6. Voer het instelwachtwoord in.
7. Als het systeem goed vanaf de diskette wordt opgestart en het systeem-ROM met succes opnieuw wordt geprogrammeerd, gaan de drie lampjes van het toetsenbord branden en klinkt bovendien een serie geluidssignalen met stijgende toonhoogte.
8. Verwijder de diskette en schakel de computer uit.
9. Schakel de computer weer in om deze opnieuw op te starten.

De onderstaande tabel laat zien welke combinaties van toetsenbordlampjes worden gebruikt door het Boot Block ROM (wanneer er een PS/2-toetsenbord op de computer is aangesloten) en wat de betekenis van deze combinaties is.

Toetsenbordlampjes voor Boot Block ROM

FailSafe Boot Block-stand	Kleur toetsenbord-lampje	Activiteit toetsenbord-lampje	Status/bericht
Num Lock	Groen	Aan	ROMPaq diskette is niet aanwezig of defect, of diskettedrive is niet gereed.
Caps Lock	Groen	Aan	Voer een wachtwoord in.
Num, Caps, Scroll Lock	Groen	Knippenen achtereenvolgens aan, één tegelijk: N, C, SL	Toetsenbord vergrendeld in netwerkstand.
Num, Caps, Scroll Lock	Groen	Aan	Boot Block ROM-flash met succes uitgevoerd. Zet de computer uit en start opnieuw op.
 Diagnoselampjes knippenen niet op USB-toetsenborden.			

Computerinstellingen kopiëren

De volgende procedure biedt een beheerder de mogelijkheid om op eenvoudige wijze een computerconfiguratie te kopiëren naar andere computers van hetzelfde type. Hierdoor kunnen meerdere computers sneller en consistenten worden geconfigureerd.



Voor beide procedures is een diskettedrive of een ondersteund USB-apparaat voor flashmedia nodig, zoals een HP Drive Key.

Kopiëren naar één computer



VOORZICHTIG: Een instellingenconfiguratie is modelspecifiek. Als de bron- en doelcomputer niet hetzelfde model zijn, kan dit leiden tot beschadiging van het bestandssysteem. Kopieer bijvoorbeeld niet de instellingenconfiguratie van een D510 Ultra-slim desktopcomputer naar een D510 e-computer.

1. Selecteer de instellingenconfiguratie die u wilt kopiëren. Zet de computer aan of start de computer opnieuw op. Klik hiervoor in Windows op **Start > Afsluiten > De computer opnieuw opstarten**.
 2. Druk op **F10** zodra het monitorlampje groen gaat branden. Druk op **Enter** om een eventueel beginscherm over te slaan.
-



Als u niet op tijd op **F10** drukt, moet u de computer uit- en vervolgens weer inschakelen en drukt u nogmaals op **F10** om het hulpprogramma te openen.

3. Plaats een diskette of een USB-apparaat voor flashmedia.
4. Klik op **File (Bestand) > Save to Diskette (Opslaan op diskette)**. Volg de instructies op het scherm voor het maken van de configuratiediskette of USB-apparaat voor flashmedia.
5. Schakel de computer die u wilt configureren uit en plaats de configuratiediskette of het USB-apparaat voor flashmedia.
6. Schakel de computer die u wilt configureren in. Druk op **F10** zodra het monitorlampje groen gaat branden. Druk op **Enter** om een eventueel beginscherm over te slaan.
7. Klik op **File (Bestand) > Restore from Diskette (Terugzetten vanaf diskette)** om de configuratie te kopiëren en volg de instructies op het scherm.
8. Start de computer opnieuw op wanneer de configuratie is voltooid.

Kopiëren naar meerdere computers



VOORZICHTIG: Een instellingenconfiguratie is modelspecifiek. Als de bron- en doelcomputer niet hetzelfde model zijn, kan dit leiden tot beschadiging van het bestandssysteem. Kopieer bijvoorbeeld niet de instellingenconfiguratie van een D510 Ultra-slim desktopcomputer naar een D510 e-computer.

Bij deze methode duurt het iets langer om de configuratiediskette of het USB-apparaat voor flashmedia gereed te maken, maar het kopiëren van de configuratie naar doelcomputers verloopt aanzienlijk sneller.



Er kan geen opstartdiskette worden gemaakt in Windows 2000. Een opstartdiskette is nodig voor deze procedure of voor het maken van een USB-apparaat voor flashmedia. Als Windows 9x of Windows XP niet beschikbaar is om een opstartdiskette te maken, gebruikt u in plaats daarvan de methode voor het kopiëren naar één computer (zie ["Kopiëren naar één computer" op pagina 10](#)).

1. Maak een opstartdiskette of een USB-apparaat voor flashmedia. Zie ["Opstartdiskette" op pagina 12](#), ["Ondersteund USB-apparaat voor flashmedia" op pagina 13](#) of ["Niet-ondersteund USB-apparaat voor flashmedia" op pagina 16](#).



VOORZICHTIG: Niet alle computers kunnen worden opgestart vanaf een USB-apparaat voor flashmedia. Als de standaard opstartvolgorde in het hulpprogramma Computer Setup (Computerinstellingen) het USB-apparaat vermeldt vóór de vaste schijf, kan de computer worden opgestart vanaf een USB-apparaat voor flashmedia. In andere gevallen moet een opstartdiskette worden gebruikt.

2. Selecteer de instellingenconfiguratie die u wilt kopiëren. Zet de computer aan of start de computer opnieuw op. Klik hiervoor in Windows op **Start > Afsluiten > De computer opnieuw opstarten**.
3. Druk op **F10** zodra het monitorlampje groen gaat branden. Druk op **Enter** om een eventueel beginscherm over te slaan.



Als u niet op tijd op **F10** drukt, moet u de computer uit- en vervolgens weer inschakelen en drukt u nogmaals op **F10** om het hulpprogramma te openen.

4. Plaats de opstartdiskette of het USB-apparaat voor flashmedia.
5. Klik op **File (Bestand) > Save to Diskette (Opslaan op diskette)**. Volg de instructies op het scherm voor het maken van de configuratiediskette of USB-apparaat voor flashmedia.
6. Download een BIOS-hulpprogramma voor het kopiëren van instellingen (repset.exe) en kopieer dit naar de configuratiediskette of het USB-apparaat voor flashmedia. Dit hulpprogramma kunt u vinden op <http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18040.html>.
7. Maak op de configuratiediskette of het USB-apparaat voor flashmedia een bestand autoexec.bat met daarin de volgende opdracht:
repset.exe
8. Schakel de computer die u wilt configureren uit. Plaats de configuratiediskette of het USB-apparaat voor flashmedia en schakel de computer in. Het configuratieprogramma wordt automatisch uitgevoerd.
9. Start de computer opnieuw op wanneer de configuratie is voltooid.

Opstartapparaat maken

Opstartdiskette



Deze instructies zijn bedoeld voor Windows XP Professional en Home Edition. Windows 2000 ondersteunt het maken van opstartdiskettes niet.

1. Plaats een diskette in de diskettedrive.
2. Klik op **Start** en vervolgens op **Deze computer**.
3. Klik met de rechtermuisknop op de diskettedrive en klik op **Formatteren**.
4. Schakel het selectievakje **Een MS-DOS-opstartdiskette maken** in en klik op **Start**.

Ga terug naar "[Kopiëren naar meerdere computers](#)" op pagina 11.

Ondersteund USB-apparaat voor flashmedia

Ondersteunde apparaten, zoals een HP Drive Key of een DiskOnKey, hebben een vooraf geïnstalleerd image waarmee het eenvoudiger wordt om er een apparaat van te maken waarvan kan worden opgestart. Als de Drive Key die wordt gebruikt dit image niet heeft, voert u de procedure verderop in dit gedeelte uit (zie [“Niet-ondersteund USB-apparaat voor flashmedia” op pagina 16](#)).



VOORZICHTIG: Niet alle computers kunnen worden opgestart vanaf een USB-apparaat voor flashmedia. Als de standaard opstartvolgorde in het hulpprogramma Computer Setup (Computerinstellingen) het USB-apparaat vermeldt vóór de vaste schijf, kan de computer worden opgestart vanaf een USB-apparaat voor flashmedia. In andere gevallen moet een opstartdiskette worden gebruikt.

Om een USB-apparaat voor flashmedia te kunnen gebruiken als opstartapparaat heeft u het volgende nodig:

■ Een van de volgende computers:

- ☐ Compaq Evo D510 Ultra-slim desktopcomputer
- ☐ Compaq Evo D510 Convertible Minitower/Small Form Factor
- ☐ HP Compaq Business Desktop d530 Serie – Ultra-slim desktopcomputer, Small Form Factor of Convertible Minitower
- ☐ Compaq Evo N400c, N410c, N600c, N610c, N620c, N800c of N1000c notebookcomputer
- ☐ Compaq Presario 1500 of 2800 notebookcomputer

Afhankelijk van het specifieke BIOS-systeem, kunnen toekomstige computers mogelijk ook het opstarten vanaf de HP Drive Key ondersteunen.



VOORZICHTIG: Als u een andere computer dan de bovenstaande gebruikt, moet u ervoor zorgen dat de standaard opstartvolgorde in het hulpprogramma Computer Setup (Computerinstellingen) het USB-apparaat vóór de vaste schijf vermeldt.

- Een van de volgende opslagmodules:
 - ☐ 16-MB HP Drive Key
 - ☐ 32-MB HP Drive Key
 - ☐ 32-MB DiskOnKey
 - ☐ 64-MB HP Drive Key
 - ☐ 64-MB DiskOnKey
 - ☐ 128-MB HP Drive Key
 - ☐ 128-MB DiskOnKey
- Een DOS-opstartdiskette met de programma's FDISK en SYS. Als SYS niet beschikbaar is, kan FORMAT worden gebruikt, maar alle bestaande bestanden op de Drive Key gaan dan verloren.
 1. Zet de computer uit.
 2. Plaats de Drive Key in een van de USB-poorten van de computer en verwijder alle overige USB-opslagapparaten, met uitzondering van USB-diskettedrives.
 3. Plaats een DOS-opstartdiskette met FDISK.COM en hetzij SYS.COM, hetzij FORMAT.COM in een diskettedrive en schakel de computer in om op te starten vanaf de DOS-diskette.
 4. Voer FDISK uit vanaf de A:\-prompt door **FDISK** te typen en op Enter te drukken. Klik desgevraagd op **Yes (Y) (Ja, J)** om ondersteuning voor grote schijfeenheden in te schakelen.
 5. Open keuzemogelijkheid **[5]** om de schijfeenheden in het systeem weer te geven. De Drive Key is de schijfeenheid die het meeste overeenkomt met de capaciteit van een van de vermelde schijfeenheden. Dit zal gewoonlijk de laatste in de lijst zijn. Noteer de schijfaanduiding.
Drive Key-drive: _____



VOORZICHTIG: Als geen van de schijfeenheden overeenkomt met de Drive Key, moet u niet doorgaan. Als u dit wel doet, kan er gegevensverlies optreden. Controleer alle USB-poorten op andere opslagapparaten. Als u deze vindt, verwijdert u ze, start u de computer opnieuw op en gaat u door vanaf stap 4. Als er geen worden gevonden, ondersteunt het systeem de Drive Key niet of is de Drive Key defect. GA NIET DOOR met het maken van de opstart-Drive Key.

6. Sluit FDISK af door op **Esc** te drukken om terug te keren naar de A:\-prompt.

7. Als de DOS-opstartdiskette SYS.COM bevat, gaat u naar stap 8. Ga anders naar stap 9.
8. Voer achter de A:\-prompt **SYS x:** in, waarbij de x de schijfaanduiding weergeeft die u hierboven heeft genoteerd. Ga naar stap 13.



VOORZICHTIG: Zorg ervoor dat u de juiste schijfaanduiding invoert voor de Drive Key.

Wanneer de systeembestanden zijn overgezet, keert SYS terug naar de A:\-prompt.

9. Kopieer alle bestanden die u wilt behouden van de Drive Key naar een tijdelijke directory op een andere schijf eenheid (bijvoorbeeld de interne vaste schijf van het systeem).
10. Voer achter de A:\-prompt **FORMAT /S X:** in, waarbij de X de schijfaanduiding weergeeft die u hierboven heeft genoteerd.



VOORZICHTIG: Zorg ervoor dat u de juiste schijfaanduiding invoert voor de Drive Key.

In het programma FORMAT worden een of meer waarschuwingen weergegeven en wordt u telkens gevraagd of u door wilt gaan. Voer telkens **y (i)** in. Met FORMAT formatteert u de Drive Key, voegt u de systeembestanden toe en wordt u gevraagd om een volumenaam.

11. Druk op **Enter** als u geen naam wilt, of voer er desgewenst een in.
12. Kopieer alle bestanden die u bij stap 9 heeft opgeslagen weer terug naar de Drive Key.
13. Verwijder de diskette en start de computer opnieuw op. De computer start op vanaf de Drive Key als drive C.



De standaard opstartvolgorde varieert van computer tot computer. Deze kan worden gewijzigd in het hulpprogramma Computer Setup (Computerinstellingen).

Als u een DOS-versie heeft gebruikt uit Windows 9x, ziet u mogelijk kort het Windows-logoscherm. Als u dit scherm niet wilt zien, voegt u een bestand met de lengte nul en de naam LOGO.SYS toe aan de hoofddirectory van de Drive Key.

Ga terug naar ["Kopiëren naar meerdere computers"](#) op pagina 11.

Niet-ondersteund USB-apparaat voor flashmedia



VOORZICHTIG: Niet alle computers kunnen worden opgestart vanaf een USB-apparaat voor flashmedia. Als de standaard opstartvolgorde in het hulpprogramma Computer Setup (Computerinstellingen) het USB-apparaat vermeldt vóór de vaste schijf, kan de computer worden opgestart vanaf een USB-apparaat voor flashmedia. In andere gevallen moet een opstartdiskette worden gebruikt.

Om een USB-apparaat voor flashmedia te kunnen gebruiken als opstartapparaat u het volgende nodig:

- Een van de volgende computers:
 - ☐ Compaq Evo D510 Ultra-slim desktopcomputer
 - ☐ Compaq Evo D510 Convertible Minitower/Small Form Factor
 - ☐ HP Compaq Business Desktop d530 Serie – Ultra-slim desktopcomputer, Small Form Factor of Convertible Minitower
 - ☐ Compaq Evo N400c, N410c, N600c, N610c, N620c, N800c of N1000c notebookcomputer
 - ☐ Compaq Presario 1500 of 2800 notebookcomputer
- Afhankelijk van het specifieke BIOS-systeem, kunnen toekomstige computers mogelijk ook het opstarten vanaf een USB-apparaat voor flashmedia.



VOORZICHTIG: Als u een andere computer dan de bovenstaande gebruikt, moet u ervoor zorgen dat de standaard opstartvolgorde in het hulpprogramma Computer Setup (Computerinstellingen) het USB-apparaat vóór de vaste schijf vermeldt.

- Een DOS-opstartdiskette met de programma's FDISK en SYS. Als SYS niet beschikbaar is, kan FORMAT worden gebruikt, maar alle bestaande bestanden op de Drive Key gaan dan verloren.
 1. Als er PCI-kaarten in het systeem aanwezig zijn waarop SCSI-, ATA RAID- of SATA-drives zijn aangesloten, schakelt u de computer uit en koppelt u het netsnoer los.



VOORZICHTIG: Het netsnoer MOET worden losgekoppeld.

2. Open de computer en verwijder de PCI-kaarten.

3. Plaats het USB-apparaat voor flashmedia in een van de USB-poorten van de computer en verwijder alle overige USB-opslagapparaten, met uitzondering van USB-diskettedrives. Sluit de kap van de computer.
4. Steek de stekker weer in het stopcontact en zet de computer aan. Zodra het monitorlampje groen gaat branden, drukt u op **F10** om het hulpprogramma Computer Setup (Computerinstellingen) te starten.
5. Ga naar Advanced/PCI devices (Geavanceerd/PCI-apparaten) om zowel de IDE- als de SATA-controllers uit te schakelen. Wanneer u de SATA-controller uitschakelt, noteert u de IRQ waaraan de controller is toegewezen. U moet de IRQ later weer toewijzen. Sluit het programma af en bevestig daarbij de wijzigingen.
SATA-IRQ: _____
6. Plaats een DOS-opstartdiskette met FDISK.COM en hetzij SYS.COM, hetzij FORMAT.COM in een diskettedrive en schakel de computer in om op te starten vanaf de DOS-diskette.
7. Voer FDISK uit en verwijder alle bestaande partities op het USB-apparaat voor flashmedia. Maak een nieuwe partitie en markeer deze als actief. Sluit FDISK af door op **Esc** te drukken.
8. Als het systeem niet automatisch opnieuw start wanneer u FDISK afsluit, drukt u op **Ctrl+Alt+Del** om opnieuw op te starten vanaf de DOS-diskette.
9. Typ achter de A:\-prompt **FORMAT C: /S** en druk op **Enter**. Met FORMAT formatteert u het USB-apparaat voor flashmedia, voegt u de systeembestanden toe en wordt u gevraagd om een volumenaam.
10. Druk op **Enter** als u geen naam wilt, of voer er desgewenst een in.
11. Schakel de computer uit en koppel het netsnoer los. Open de computer en installeer opnieuw de PCI-kaarten die u eerder heeft verwijderd. Sluit de kap van de computer.
12. Steek de stekker weer in het stopcontact, verwijder de diskette en zet de computer aan.
13. Zodra het monitorlampje groen gaat branden, drukt u op **F10** om het hulpprogramma Computer Setup (Computerinstellingen) te starten.

14. Ga naar Advanced/PCI Devices (Geavanceerd/PCI-apparaten) en schakel de IDE- en SATA-controllers die in stap 5 werden uitgeschakeld weer in. Plaats de SATA-controller terug op de oorspronkelijke IRQ.
15. Sla de wijzigingen op en sluit af. De computer start op vanaf het USB-apparaat voor flashmedia als drive C.



De standaard opstartvolgorde varieert van computer tot computer. Deze kan worden gewijzigd in het hulpprogramma Computer Setup (Computerinstellingen).

Als u een DOS-versie heeft gebruikt uit Windows 9x, ziet u mogelijk kort het Windows-logoscherm. Als u dit scherm niet wilt zien, voegt u een bestand met de lengte nul en de naam LOGO.SYS toe aan de hoofddirectory van de Drive Key.

Ga terug naar "[Kopiëren naar meerdere computers](#)" op pagina 11.

Aan/uit-knop met twee standen

Als ACPI (Advanced Configuration and Power Interface) is ingeschakeld voor Windows 2000 of Windows XP Professional en Home Edition, kan de aan/uit-knop functioneren als een aan/uit-schakelaar of als een standbyknop. In de standbystand wordt de voeding niet helemaal afgesloten maar verbruikt de computer minder energie. Hierdoor kunt u snel het stroomverbruik beperken zonder dat u applicaties hoeft te sluiten en kan de computer snel naar de oorspronkelijke stand terugkeren zonder dat u gegevens verliest.

U wijzigt de configuratie van de aan/uit-knop als volgt:

1. In Windows 2000 klikt u op **Start** en vervolgens selecteert u **Instellingen > Configuratiescherm > Energiebeheer**.

In Windows XP Professional en Home Edition klikt u op **Start** en vervolgens selecteert u **Configuratiescherm > Prestaties en onderhoud > Energiebeheer**.

2. Selecteer het tabblad **Geavanceerd** in het venster **Eigenschappen voor Energiebeheer**.

3. Selecteer in het gedeelte **Aan/uit-knop** de gewenste instelling voor de aan/uit-knop.

Als u de aan/uit-knop eenmaal heeft geconfigureerd als standbyknop, kunt u met deze knop overschakelen op een stand met een bijzonder laag energieverbruik. Druk nogmaals op deze knop om weer terug te gaan naar de maximale stroomvoorziening. Als u de stroomvoorziening helemaal wilt uitschakelen, houdt u de aan/uit-knop vier seconden ingedrukt.



VOORZICHTIG: Gebruik de aan/uit-knop niet om de computer uit te schakelen, tenzij het systeem niet meer reageert. Als u de stroomtoevoer uitschakelt zonder tussenkomst van het besturingssysteem, kunnen er gegevens op de vaste schijf beschadigd raken of verloren gaan.

Website

HP verzorgt grondige tests en debugprocedures van software die door HP of andere leveranciers wordt ontwikkeld. Bovendien ontwikkelt HP ondersteunende software specifiek voor elk besturingssysteem, zodat HP computers optimaal presteren op het gebied van snelheid, compatibiliteit en betrouwbaarheid.

Wanneer u overschakelt naar een ander besturingssysteem of naar een nieuwere versie van het besturingssysteem, is het belangrijk om de ondersteunende software te implementeren die is ontwikkeld voor het betreffende besturingssysteem of de betreffende versie. Als u een andere versie van Microsoft Windows wilt gebruiken dan de versie die bij de computer is geleverd, is het noodzakelijk dat u de overeenkomstige stuurprogramma's en hulpprogramma's installeert, zodat alle voorzieningen worden ondersteund en naar behoren functioneren.

Het is heel eenvoudig om de meest recente versies van de ondersteunende software van HP te vinden, te verkrijgen, uit te proberen en te installeren. U kunt de software downloaden vanaf <http://www.hp.com/support>.

De websites bevatten de meest recente versie van stuurprogramma's, hulpprogramma's en flash-ROM-images die nodig zijn om het meest recente Microsoft Windows-besturingssysteem op de HP computer te gebruiken.

Bouwstenen en partners

De HP oplossingen voor systeembeheer kunnen goed worden geïntegreerd met andere applicaties voor systeembeheer en zijn gebaseerd op industriestandaarden, zoals:

- Desktop Management Interface (DMI) 2.0
- Wake on LAN
- ACPI
- SMBIOS
- PXE-ondersteuning (Pre-boot Execution)

Inventarisbeheer en beveiliging

Ingebouwde functies voor inventarisbeheer leveren essentiële inventarisgegevens op, die kunnen worden beheerd met HP Insight Manager, HP Client Manager of andere applicaties voor systeembeheer. Dankzij de naadloze, automatische integratie van de voorzieningen voor inventarisbeheer met deze producten, kunt u een hulpprogramma voor computerbeheer kiezen dat het beste aansluit op de omgeving, zodat de investering in bestaande software zijn waarde behoudt.

HP biedt ook mogelijkheden om de toegang tot waardevolle onderdelen en informatie te beveiligen. Indien Embedded Security van ProtectTools is geïnstalleerd, voorkomt dit ongevoegde toegang tot gegevens, wordt de systeemintegriteit gecontroleerd en worden pogingen van derden om toegang te krijgen tot het systeem geverifieerd. Met behulp van beveiligingsvoorzieningen als ProtectTools, Smart Cover Sensor en Smart Cover Lock, die op bepaalde modellen beschikbaar zijn, kunt u ongeoorloofde toegang tot de interne onderdelen van de computer voorkomen. Door parallelle poorten, seriële poorten of USB-poorten uit te schakelen of door het onmogelijk te maken om de computer op te starten vanaf een verwisselbare schijf eenheid, kunt u waardevolle gegevens beschermen. Waarschuwingen bij geheugenwijzigingen en waarschuwingen van de Smart Cover Sensor kunnen automatisch worden doorgestuurd naar applicaties voor systeembeheer, zodat geknoei met de interne onderdelen van een computer vroegtijdig wordt gemeld.




Op bepaalde systemen zijn Protect Tools, de Smart Cover Sensor en het Smart Cover Lock als optie leverbaar.

Er zijn verschillende manieren waarop beveiligingsinstellingen op HP computers kunnen worden beheerd:

- Lokaal, met het hulpprogramma Computerinstellingen. Zie de *Handleiding Computer Setup (Computerinstellingen)* voor aanvullende informatie en instructies voor het gebruik van het hulpprogramma Computer Setup (Computerinstellingen).
- Op afstand, met HP Client Manager of System Software Manager (SSM). SSM biedt veilige, consistente implementatie en besturing van beveiligingsinstellingen met behulp van een eenvoudig hulpprogramma.

In de volgende tabel en gedeelten vindt u informatie over het lokale beheer van beveiligingsvoorzieningen op de computer via het hulpprogramma Computer Setup (Computerinstellingen).

Overzicht van beveiligingsvoorzieningen

Voorziening	Functie	Instellen
Opstartbeveiliging verwisselbare schijfeenheden	Voorkomt opstarten vanaf de verwisselbare schijfeenheden. (beschikbaar op bepaalde drives)	Vanuit Computer Setup (Computerinstellingen).
Beveiliging parallelle, seriële, USB- en infraroodpoorten	Voorkomt gegevensoverdracht via de geïntegreerde seriële en parallelle poort en de USB- en infraroodpoort.	Vanuit Computer Setup (Computerinstellingen).
Power-On Password (Opstartwachtwoord)	Voorkomt dat de computer kan worden gebruikt als het wachtwoord niet is ingevoerd. Dit kan zowel van toepassing zijn bij het eerste opstarten van het systeem als bij het opnieuw starten.	Vanuit Computer Setup (Computerinstellingen).
 Raadpleeg de <i>Handleiding Computer Setup (Computerinstellingen)</i> voor meer informatie over Computer Setup (Computerinstellingen). Welke beveiligingsopties precies worden ondersteund, is afhankelijk van de computerconfiguratie.		

Overzicht van beveiligingsvoorzieningen *(Vervolg)*


Voorziening	Functie	Instellen
Setup Password (Instelwachtwoord)	Voorkomt dat de configuratie wordt gewijzigd (via Computerinstellingen), tenzij het wachtwoord wordt ingevoerd.	Vanuit Computer Setup (Computerinstellingen).
Embedded Security Device (Geïntegreerd beveiligingsapparaat)	Hiermee voorkomt u onbevoegde toegang tot gegevens met behulp van codering en wachtwoordbeveiliging. De systeemintegriteit wordt gecontroleerd en pogingen van derden om toegang te krijgen tot het systeem worden geverifieerd.	Vanuit Computer Setup (Computerinstellingen).
DriveLock	Beschermt gegevens op MultiBay vaste schijven tegen onbevoegd gebruik. Deze functie is niet op alle modellen beschikbaar.	Vanuit Computer Setup (Computerinstellingen).




Raadpleeg de *Handleiding Computer Setup (Computerinstellingen)* voor meer informatie over Computer Setup (Computerinstellingen).

Welke beveiligingsopties precies worden ondersteund, is afhankelijk van de computerconfiguratie.

Overzicht van beveiligingsvoorzieningen (Vervolg)

Voorziening	Functie	Instellen
Smart Cover Sensor	Geeft aan dat de kap of het zijpaneel van de computer is verwijderd. U kunt deze optie zo instellen dat de gebruiker het instelwachtwoord moet invoeren om de computer opnieuw te kunnen opstarten nadat de kap of het zijpaneel is verwijderd. Raadpleeg de <i>Handleiding voor de hardware op de cd Documentation Library</i> voor meer informatie. Deze functie is niet op alle modellen beschikbaar.	Vanuit Computer Setup (Computerinstellingen).
MBR-beveiliging	Kan onbedoelde of opzettelijke wijzigingen in de hoofdopstartrecord (Master Boot Record, MBR) van de huidige opstartschijf voorkomen en maakt herstel van de vorige, ongewijzigde MBR mogelijk.	Vanuit Computer Setup (Computerinstellingen).
Waarschuwingen bij geheugenwijziging	Detecteert wanneer geheugenmodules zijn toegevoegd, verplaatst of verwijderd en stelt zowel de eindgebruiker als de systeembeheerder op de hoogte.	Raadpleeg de online handleiding <i>Intelligent Manageability</i> voor informatie over het inschakelen van waarschuwingen bij geheugenwijzigingen.
 Raadpleeg de <i>Handleiding Computer Setup (Computerinstellingen)</i> voor meer informatie over Computer Setup (Computerinstellingen). Welke beveiligingsopties precies worden ondersteund, is afhankelijk van de computerconfiguratie.		

Overzicht van beveiligingsvoorzieningen (Vervolg)

Voorziening	Functie	Instellen
Eigendomslabel	Toont de door de systeembeheerder vastgelegde eigendomsinformatie tijdens het opstarten van de computer (beschermd met het instelwachtwoord).	Vanuit Computer Setup (Computerinstellingen).
Voorziening voor een kabelslot	Een kabelslot voorkomt dat onbevoegden toegang hebben tot de binnenkant van de computer en zo de configuratie kunnen wijzigen of onderdelen kunnen verwijderen. U kunt deze voorziening ook gebruiken om de computer met een kabelslot vast te leggen aan een moeilijk verplaatsbaar object, ter voorkoming van diefstal.	Bevestig de computer met een kabelslot aan een moeilijk verplaatsbaar object.
Voorziening voor een hangslot	Een hangslot voorkomt dat onbevoegden toegang hebben tot de binnenkant van de computer en zo de configuratie kunnen wijzigen of onderdelen kunnen verwijderen.	Installeer een slot in de beveiligingslus om ongewenste configuratiewijzigingen of verwijdering van componenten te voorkomen.
 Raadpleeg de <i>Handleiding Computer Setup (Computerinstellingen)</i> voor meer informatie over Computer Setup (Computerinstellingen). Welke beveiligingsopties precies worden ondersteund, is afhankelijk van de computerconfiguratie.		

Wachtwoordbeveiliging

Het opstartwachtwoord voorkomt dat onbevoegden de computer kunnen gebruiken. Telkens wanneer een gebruiker de computer inschakelt of opnieuw opstart, moet deze een wachtwoord invoeren om toegang te krijgen tot applicaties of gegevens. Het instelwachtwoord voorkomt specifiek onbevoegde toegang tot Computer Setup (Computerinstellingen) en kan ook worden gebruikt om het opstartwachtwoord te negeren. Dit betekent dat als u het instelwachtwoord invoert wanneer om het opstartwachtwoord wordt gevraagd, u toch toegang krijgt tot de computer.

Er kan een voor het hele netwerk geldig instelwachtwoord worden ingesteld om de systeembeheerder in staat te stellen zich aan te melden op alle netwerksystemen om onderhoud uit te voeren, zonder het opstartwachtwoord te hoeven kennen, ook al is er een ingesteld.

Instelwachtwoord definiëren met Computer Setup (Computerinstellingen)

Als het systeem voorzien is van een geïntegreerd beveiligingsapparaat, raadpleegt u [“Embedded Security \(Geïntegreerde beveiliging\)” op pagina 31](#).

U kunt een instelwachtwoord definiëren met behulp van Computer Setup (Computerinstellingen). Zo voorkomt u dat de configuratie (via Computerinstellingen) wordt gewijzigd zonder dat het wachtwoord wordt ingevoerd.

1. Zet de computer aan of start de computer opnieuw op. Klik hiervoor in Windows op **Start > Afsluiten > De computer opnieuw opstarten**.
2. Druk op **F10** zodra het monitorlampje groen gaat branden. Druk op **Enter** om een eventueel beginscherm over te slaan.



Als u niet op tijd op **F10** drukt, moet u de computer uit- en vervolgens weer inschakelen en drukt u nogmaals op **F10** om het hulpprogramma te openen.

3. Selecteer achtereenvolgens **Security (Beveiliging)** en **Setup Password (Instelwachtwoord)** en volg de instructies op het scherm.
4. Klik op **File (Bestand) > Save Changes and Exit (Wijzigingen opslaan en afsluiten)** voordat u het programma afsluit.

Opstartwachtwoord definiëren met Computer Setup (Computerinstellingen)

Het opstartwachtwoord is een beveiligingsvoorziening waarmee de computer alleen kan worden gebruikt als eerst een wachtwoord wordt ingevoerd. Als u een opstartwachtwoord heeft ingesteld, verschijnt de opdracht Password Options (Wachtwoordopties) in het menu Security (Beveiliging). Een van de wachtwoordopties is Password Prompt on Warm Boot (Wachtwoordprompt bij warme start). Als Password Prompt on Warm Boot is ingeschakeld, moet u het wachtwoord ook invoeren telkens wanneer u de computer opnieuw opstart.

1. Zet de computer aan of start de computer opnieuw op. Klik hiervoor in Windows op **Start > Afsluiten > De computer opnieuw opstarten**.
2. Druk op **F10** zodra het monitorlampje groen gaat branden.
Druk op **Enter** om een eventueel beginscherm over te slaan.



Als u niet op tijd op **F10** drukt, moet u de computer uit- en vervolgens weer inschakelen en drukt u nogmaals op **F10** om het hulpprogramma te openen.

3. Selecteer achtereenvolgens **Security (Beveiliging)** en **Power-On Password (Opstartwachtwoord)** en volg de instructies op het scherm.
4. Klik op **File (Bestand) > Save Changes and Exit (Wijzigingen opslaan en afsluiten)** voordat u het programma afsluit.

Opstartwachtwoord invoeren

U voert als volgt een opstartwachtwoord in:

1. Zet de computer aan of start de computer opnieuw op. Klik hiervoor in Windows op **Start > Afsluiten > De computer opnieuw opstarten**.
2. Wanneer het sleutelpictogram op het beeldscherm verschijnt, typt u het huidige wachtwoord en drukt u op **Enter**.



Typ zorgvuldig. Uit veiligheidsoverwegingen worden de tekens die u typt niet op het scherm weergegeven.

Als u het wachtwoord verkeerd invoert, verschijnt het pictogram van een gebroken sleutel. Probeer het opnieuw. Na drie mislukte pogingen moet u de computer uitzetten en opnieuw opstarten voordat u verder kunt.

Instelwachtwoord invoeren

Als het systeem voorzien is van een geïntegreerd beveiligingsapparaat, raadpleegt u [“Embedded Security \(Geïntegreerde beveiliging\)” op pagina 31](#).

Als er een instelwachtwoord op de computer is gedefinieerd, wordt u gevraagd dit in te voeren wanneer u Computer Setup (Computerinstellingen) wilt uitvoeren.

1. Zet de computer aan of start de computer opnieuw op. Klik hiervoor in Windows op **Start > Afsluiten > De computer opnieuw opstarten**.
2. Druk op **F10** zodra het monitorlampje groen gaat branden.



Als u niet op tijd op **F10** drukt, moet u de computer uit- en vervolgens weer inschakelen en drukt u nogmaals op **F10** om het hulpprogramma te openen.

3. Wanneer het sleutelpictogram op het beeldscherm verschijnt, typt u het instelwachtwoord en drukt u op **Enter**.



Typ zorgvuldig. Uit veiligheidsoverwegingen worden de tekens die u typt niet op het scherm weergegeven.

Als u het wachtwoord verkeerd invoert, verschijnt het pictogram van een gebroken sleutel. Probeer het opnieuw. Na drie mislukte pogingen moet u de computer uitzetten en opnieuw opstarten voordat u verder kunt.

Opstart- of instelwachtwoord wijzigen

Als het systeem voorzien is van een geïntegreerd beveiligingsapparaat, raadpleegt u “[Embedded Security \(Geïntegreerde beveiliging\)](#)” op pagina 31.

1. Zet de computer aan of start de computer opnieuw op. Klik hiervoor in Windows op **Start > Afsluiten > De computer opnieuw opstarten**. Start **Computer Setup (Computerinstellingen)** om het instelwachtwoord te wijzigen.
2. Voer als het sleutelpictogram verschijnt het huidige wachtwoord in, gevolgd door een schuine streep (/) of een ander scheidingsteken, het nieuwe wachtwoord, nog een schuine streep (/) of een ander scheidingsteken en ten slotte nogmaals het nieuwe wachtwoord, zoals hieronder wordt weergegeven:
**huidig wachtwoord/nieuw wachtwoord/
nieuw wachtwoord**



Typ zorgvuldig. Uit veiligheidsoverwegingen worden de tekens die u typt niet op het scherm weergegeven.

3. Druk op **Enter**.

Het nieuwe wachtwoord wordt van kracht als u de computer opnieuw aan zet.



Raadpleeg “[Scheidingstekens en landspecifieke toetsenborden](#)” op pagina 30 voor informatie over de andere scheidingstekens. U kunt het opstartwachtwoord en het instelwachtwoord ook wijzigen met behulp van de beveiligingsopties in Computer Setup (Computerinstellingen).

Opstart- of instelwachtwoord verwijderen

Als het systeem voorzien is van een geïntegreerd beveiligingsapparaat, raadpleegt u “[Embedded Security \(Geïntegreerde beveiliging\)](#)” op pagina 31.

1. Zet de computer aan of start de computer opnieuw op. Klik hiervoor in Windows op **Start > Afsluiten > De computer opnieuw opstarten**. Start **Computer Setup (Computerinstellingen)** om het instelwachtwoord te verwijderen.
2. Voer als het sleutelpictogram verschijnt het huidige wachtwoord in, gevolgd door een schuine streep (/) of een ander scheidingsteken, zoals hieronder wordt weergegeven:
huidig wachtwoord/
3. Druk op **Enter**.



Raadpleeg “[Scheidingstekens en landspecifieke toetsenborden](#)” voor informatie over de andere scheidingstekens. U kunt het opstartwachtwoord en het instelwachtwoord ook wijzigen met behulp van de beveiligingsopties in Computer Setup (Computerinstellingen).

Scheidingstekens en landspecifieke toetsenborden

Elk toetsenbord is ontworpen om tegemoet te komen aan landspecifieke vereisten. De syntaxis en de toetsen die u gebruikt om een wachtwoord te wijzigen of te verwijderen zijn afhankelijk van het toetsenbord dat bij de computer is geleverd. In Nederland wordt meestal gebruikgemaakt van het toetsenbord VS/Internationaal.

Scheidingstekens en landspecifieke toetsenborden

Arabisch	/	Grieks	-	Russisch	/
Belgisch	=	Hebreeuws	.	Slowaaks	-
BHKSJ*	-	Hongaars	-	Spaans	-
Braziliaans	/	Italiaans	-	Zweeds/Fins	/
Chinees	/	Japans	/	Zwitsers	-
Tsjechisch	-	Koreaans	/	Taiwanees	/
Deens	-	Latijns-Amerikaans	-	Thais	/
Frans	!	Noors	-	Turks	.
Canadees (Frans)	é	Pools	-	Engels (GB)	/
Duits	-	Portugees	-	VS/Internationaal	/

* Voor Bosnië-Herzegovina, Kroatië, Slovenië en Joegoslavië.

Wachtwoorden wissen

Als u het wachtwoord bent vergeten, heeft u geen toegang tot de computer. Raadpleeg de handleiding *Problemen oplossen* voor informatie over het wissen van wachtwoorden.

Als het systeem voorzien is van een geïntegreerd beveiligingsapparaat, raadpleegt u [“Embedded Security \(Geïntegreerde beveiliging\).”](#)

Embedded Security (Geïntegreerde beveiliging)

ProtectTools Embedded Security maakt gebruik van een combinatie van codering en wachtwoordbeveiliging om uitgebreide beveiliging te bieden voor EFS (Embedded File System) bestands/map-codering en veilige e-mailberichten bij Microsoft Outlook en Outlook Express. ProtectTools is beschikbaar voor bepaalde zakelijke desktopcomputers als optie die op bestelling wordt geconfigureerd. Deze optie is bedoeld voor gebruikers van HP systemen voor wie de veiligheid van gegevens van het allergrootste belang is: Onbevoegde toegang tot gegevens vormt een veel groter gevaar dan het verlies van gegevens. ProtectTools maakt gebruik van vier wachtwoorden:

- (F10) Setup (Instelwachtwoord): voor toegang tot het hulpprogramma Computer Setup (Computerinstellingen) en het in- en uitschakelen van ProtectTools;
- Take Ownership (Eigendom verkrijgen): in te stellen en te gebruiken door een systeembeheerder, die gebruikers toegangsrechten geeft en beveiligingsparameters instelt;
- Emergency Recovery Token (Noodhersteltoken): in te stellen door de systeembeheerder, maakt herstel mogelijk bij uitval van de computer of de ProtectTools-chip;
- Basic User (Basisgebruiker): in te stellen en te gebruiken door de eindgebruiker.



Als het wachtwoord van de eindgebruiker verloren raakt, kunnen gecodeerde gegevens niet worden hersteld. Daarom wordt u aangeraden bij het gebruik van ProtectTools de gegevens op de vaste schijf van de gebruiker te kopiëren op een bedrijfsinformatiesysteem of er regelmatig een backup van te maken.

ProtectTools Embedded Security is een beveiligingschip die voldoet aan TCPA 1.1 en optioneel wordt geïnstalleerd op de systeemkaart van bepaalde zakelijke desktopcomputers. Elke ProtectTools Embedded Security-chip is uniek en gekoppeld aan een specifieke computer. Elke chip voert belangrijke beveiligingsprocessen uit, onafhankelijk van andere computeronderdelen (zoals de processor, het geheugen of het besturingssysteem).

Een computer waarop ProtectTools Embedded Security is ingeschakeld heeft daarmee een aanvulling op de beveiligingsmogelijkheden die zijn ingebouwd in Microsoft Windows 2000 of Windows XP Professional of Home Edition. Het besturingssysteem kan bijvoorbeeld lokale bestanden en mappen coderen op basis van EFS, maar ProtectTools Embedded Security biedt een extra beveiligingslaag door coderingssleutels te maken op basis van de hoofdsleutel (die is vastgelegd in silicium). Dit proces wordt “wrapping” (inpakken) van coderingssleutels genoemd. ProtectTools voorkomt niet dat via een netwerk toegang wordt verkregen tot een computer zonder ProtectTools.

De belangrijkste mogelijkheden van ProtectTools Embedded Security zijn:

- Platformverificatie
- Beschermd opslag
- Gegevensintegriteit



VOORZICHTIG: Ga zorgvuldig om met de wachtwoorden. **Gecodeerde gegevens zijn niet toegankelijk en kunnen niet worden hersteld zonder de wachtwoorden.**

Wachtwoorden instellen

Instelwachtwoord

Er kan een instelwachtwoord worden vastgelegd en het geïntegreerde beveiligingsapparaat kan worden ingeschakeld met F10 voor het hulpprogramma Computer Setup (Computerinstellingen).

1. Druk op **F10** zodra het monitorlampje groen gaat branden.



Als u niet op tijd op **F10** drukt, moet u de computer uit- en vervolgens weer inschakelen en drukt u nogmaals op **F10** om het hulpprogramma te openen.

2. Selecteer met de pijl-omhoog of pijl-omlaag een taal en druk op **Enter**.
3. Ga met behulp van de pijl-links of pijl-rechts naar het tabblad **Security (Beveiliging)** en ga met de pijl-omhoog of pijl-omlaag naar **Setup Password (Instelwachtwoord)**. Druk op **Enter**.

4. Typ en bevestig het wachtwoord. Druk op **F10** om het wachtwoord te accepteren.



Typ zorgvuldig. Uit veiligheidsoverwegingen worden de tekens die u typt niet op het scherm weergegeven.

5. Ga met de pijl-omhoog of pijl-omlaag naar **Embedded Security Device (Geïntegreerd beveiligingsapparaat)**. Druk op **Enter**.
6. Als de selectie in het dialoogvenster **Embedded Security Device – Disable (Geïntegreerd beveiligingsapparaat – Uitschakelen)** is, wijzigt u dit met de pijl-links of pijl-rechts in **Embedded Security Device – Enable (Geïntegreerd beveiligingsapparaat – Inschakelen)**. Druk op **F10** om de wijziging te accepteren.



VOORZICHTIG: Als u **Reset to Factory Settings – Reset (Fabrieksinstellingen herstellen – Opnieuw instellen)** selecteert, worden alle sleutels gewist en kunnen gecodeerde gegevens niet worden hersteld *tenzij* van de sleutels een backup is gemaakt (zie [“Wachtwoorden voor Take Ownership \(Eigendom verkrijgen\) en Emergency Recovery Token \(Noodhersteltoken\)”](#)). Selecteer **Reset (Opnieuw instellen)** alleen wanneer hierom wordt gevraagd in de procedure voor het herstellen van gecodeerde gegevens (zie [“Gecodeerde gegevens herstellen” op pagina 36](#)).

7. Ga met de pijl-links of pijl-rechts naar **File (Bestand)**. Ga met de pijl-omhoog of pijl-omlaag naar **Save Changes and Exit (Wijzigingen opslaan en afsluiten)**. Druk op **Enter** en druk ter bevestiging op **F10**.

Wachtwoorden voor Take Ownership (Eigendom verkrijgen) en Emergency Recovery Token (Noodhersteltoken)

Het Take Ownership-wachtwoord is vereist om het beveiligingsplatform in en uit te schakelen en om gebruikers toegangsrechten te geven. Als het geïntegreerde beveiligingsapparaat uitvalt, kunnen gebruikers met het noodherstelmechanisme toegangsrechten krijgen en kunnen gegevens toegankelijk worden gemaakt.

1. Als u Windows XP Professional of Home Edition gebruikt, klikt u op **Start > Alle programma's > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard**.

Als u Windows 2000 gebruikt, klikt u op **Start > Programma's > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard**.

2. Klik op **Volgende**.
3. Typ en bevestig een Take Ownership-wachtwoord en klik op **Volgende**.



Typ zorgvuldig. Uit veiligheidsoverwegingen worden de tekens die u typt niet op het scherm weergegeven.

4. Klik op **Volgende** om de standaardlocatie voor het herstelarchief te accepteren.
5. Typ en bevestig een Emergency Recovery Token-wachtwoord en klik op **Volgende**.
6. Plaats een diskette in de diskettedrive om hierop de Emergency Recovery Token-sleutel op te slaan. Klik op **Bladeren** en selecteer de diskettedrive.



VOORZICHTIG: De Emergency Recovery Token-sleutel wordt gebruikt om gecodeerde gegevens te herstellen in het geval van uitval van een computer of de geïntegreerde beveiligingschip. **Zonder de sleutel kunnen geen gegevens worden hersteld.** (De gegevens zijn nog steeds niet toegankelijk zonder het basisgebruikerswachtwoord.) Bewaar deze diskette op een veilige plaats.

7. Klik op **Opslaan** om de locatie en de standaard bestandsnaam te accepteren en klik op **Volgende**.
8. Klik op **Volgende** om de instellingen te bevestigen voordat het beveiligingsplatform wordt geïnitieerd.



Mogelijk verschijnt er een bericht waarin wordt gemeld dat de geïntegreerde beveiligingsfuncties niet zijn geïnitieerd. Klik niet op dit bericht; dit komt later in de procedure aan bod en het bericht verdwijnt na enkele seconden.

9. Klik op **Volgende** om het configureren van het plaatselijke beleid over te slaan.
 10. Zorg ervoor dat het selectievakje Start Embedded Security User Initialization Wizard (Wizard Gebruikersinitialisatie voor geïntegreerde beveiliging starten) is ingeschakeld en klik op **Voltooiën**.
- De wizard Gebruikersinitialisatie start nu automatisch.

Basisgebruikerswachtwoord

Tijdens het initialiseren van gebruikers, wordt het Basic User Password (Basisgebruikerswachtwoord) gemaakt. Dit wachtwoord is vereist om gecodeerde gegevens in te voeren en toegankelijk te maken.



VOORZICHTIG: Ga zorgvuldig om met het basisgebruikerswachtwoord. **Zonder dit wachtwoord zijn gecodeerde gegevens niet toegankelijk en kunnen ze niet worden hersteld.**

1. Als de wizard Gebruikersinitialisatie niet open is:

Als u Windows XP Professional of Home Edition gebruikt, klikt u op **Start > Alle programma's > HP ProtectTools Embedded Security Tools > User Initialization Wizard**.

Als u Windows 2000 gebruikt, klikt u op **Start > Programma's > HP ProtectTools Embedded Security Tools > User Initialization Wizard**.

2. Klik op **Volgende**.
3. Typ en bevestig een Basic User Key-wachtwoord en klik op **Volgende**.



Typ zorgvuldig. Uit veiligheidsoverwegingen worden de tekens die u typt niet op het scherm weergegeven.

4. Klik op **Volgende** om de instellingen te bevestigen.
5. Selecteer de gewenste beveiligingsfuncties en klik op **Volgende**.
6. Klik op de juiste e-mailclient om deze te selecteren en klik op **Volgende**.
7. Klik op **Volgende** om het coderingscertificaat toe te passen.
8. Klik op **Volgende** om de instellingen te bevestigen.
9. Klik op **Voltooien**.
10. Start de computer opnieuw op.

Gecodeerde gegevens herstellen

Als u gegevens wilt herstellen na het vervangen van de ProtectTools-chip, moet u beschikken over het volgende:

- SPEmRecToken.xml: de Emergency Recovery Token-sleutel
- SPEmRecArchive.xml: verborgen map, standaardlocatie:
C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\Recovery Archive
- ProtectTools-wachtwoorden
 - ☐ Setup (Instelwachtwoord)
 - ☐ Take Ownership (Eigendom verkrijgen)
 - ☐ Emergency Recovery Token (Noodhersteltoken)
 - ☐ Basic User (Basisgebruiker)

1. Start de computer opnieuw op.
2. Druk op **F10** zodra het monitorlampje groen gaat branden.



Als u niet op tijd op **F10** drukt, moet u de computer uit- en vervolgens weer inschakelen en drukt u nogmaals op **F10** om het hulpprogramma te openen.

3. Typ het instelwachtwoord en druk op **Enter**.
4. Selecteer met de pijl-omhoog of pijl-omlaag een taal en druk op **Enter**.
5. Ga met behulp van de pijl-links of pijl-rechts naar het tabblad **Security (Beveiliging)** en ga met de pijl-omhoog of pijl-omlaag naar **Embedded Security Device (Geïntegreerd beveiligingsapparaat)**. Druk op **Enter**.
6. Als slechts één keuzemogelijkheid **Embedded Security Device – Disable (Geïntegreerd beveiligingsapparaat – Uitschakelen)** beschikbaar is:
 - a. Wijzig dit met de pijl-links of pijl-rechts in **Embedded Security Device – Enable (Geïntegreerd beveiligingsapparaat – Inschakelen)**. Druk op **F10** om de wijziging te accepteren.

b. Ga met de pijl-links of pijl-rechts naar **File (Bestand)**. Ga met de pijl-omhoog of pijl-omlaag naar **Save Changes and Exit (Wijzigingen opslaan en afsluiten)**. Druk op **Enter** en druk ter bevestiging op **F10**.

c. Ga naar stap 1.

Als er twee keuzemogelijkheden beschikbaar zijn, gaat u naar stap 7.

7. Ga met de pijl-omhoog of pijl-omlaag naar **Reset to Factory Settings – Do Not Reset (Fabrieksinstellingen herstellen – Niet opnieuw instellen)**. Druk één keer op de pijl-links of pijl-rechts.

Het volgende bericht verschijnt: Performing this action will reset the embedded security device to factory settings if settings are saved on exit. (Wanneer u deze actie uitvoert, worden de fabrieksinstellingen van het geïntegreerde beveiligingsapparaat hersteld indien de instellingen bij het afsluiten worden opgeslagen.) Druk op een toets om door te gaan.

Druk op **Enter**.

8. De geselecteerde optie is nu **Reset to Factory Settings – Reset (Fabrieksinstellingen herstellen – Opnieuw instellen)**. Druk op **F10** om de wijziging te accepteren.

9. Ga met de pijl-links of pijl-rechts naar **File (Bestand)**. Ga met de pijl-omhoog of pijl-omlaag naar **Save Changes and Exit (Wijzigingen opslaan en afsluiten)**. Druk op **Enter** en druk ter bevestiging op **F10**.

10. Start de computer opnieuw op.

11. Druk op **F10** zodra het monitorlampje groen gaat branden.



Als u niet op tijd op **F10** drukt, moet u de computer uit- en vervolgens weer inschakelen en drukt u nogmaals op **F10** om het hulpprogramma te openen.

12. Typ het instelwachtwoord en druk op **Enter**.

13. Selecteer met de pijl-omhoog of pijl-omlaag een taal en druk op **Enter**.

14. Ga met behulp van de pijl-links of pijl-rechts naar het tabblad **Security (Beveiliging)** en ga met de pijl-omhoog of pijl-omlaag naar **Embedded Security Device (Geïntegreerd beveiligingsapparaat)**. Druk op **Enter**.
15. Als de selectie in het dialoogvenster **Embedded Security Device – Disable (Geïntegreerd beveiligingsapparaat – Uitschakelen)** is, wijzigt u dit met de pijl-links of pijl-rechts in **Embedded Security Device – Enable (Geïntegreerd beveiligingsapparaat – Inschakelen)**. Druk op **F10**.
16. Ga met de pijl-links of pijl-rechts naar **File (Bestand)**. Ga met de pijl-omhoog of pijl-omlaag naar **Save Changes and Exit (Wijzigingen opslaan en afsluiten)**. Druk op **Enter** en druk ter bevestiging op **F10**.
17. Wanneer Windows is geopend:

Als u Windows XP Professional of Home Edition gebruikt, klikt u op **Start > Alle programma's > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard**.

Als u Windows 2000 gebruikt, klikt u op **Start > Programma's > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard**.
18. Klik op **Volgende**.
19. Typ en bevestig een Take Ownership-wachtwoord. Klik op **Volgende**.



Typ zorgvuldig. Uit veiligheidsoverwegingen worden de tekens die u typt niet op het scherm weergegeven.

20. Zorg dat Create a new recovery archive (Een nieuw herstelarchief maken) is geselecteerd. Klik onder **Recovery archive location (Locatie herstelarchief)** op **Bladeren**.
21. Accepteer niet de standaard bestandsnaam. Typ een nieuwe bestandsnaam, om te voorkomen dat het oorspronkelijke bestand wordt vervangen.
22. Klik op **Opslaan** en vervolgens op **Volgende**.
23. Typ en bevestig een Emergency Recovery Token-wachtwoord en klik op **Volgende**.

24. Plaats een diskette in de diskettedrive om hierop de Emergency Recovery Token-sleutel op te slaan. Klik op **Bladeren** en selecteer de diskettedrive.
25. Accepteer niet de standaard sleutelnaam. Typ een nieuwe sleutelnaam om te voorkomen dat de oorspronkelijke sleutel wordt vervangen.
26. Klik op **Opslaan** en vervolgens op **Volgende**.
27. Klik op **Volgende** om de instellingen te bevestigen voordat het beveiligingsplatform wordt geïntialiseerd.



Mogelijk verschijnt er een bericht dat de Basic User Key (Basisgebruikerssleutel) niet kan worden geladen. Klik niet op dit bericht; dit komt later in de procedure aan bod en het bericht verdwijnt na enkele seconden.

28. Klik op **Volgende** om het configureren van het plaatselijke beleid over te slaan.
29. Klik op het selectievakje **Start Embedded Security User Initialization Wizard (Wizard Gebruikersinitialisatie voor geïntegreerde beveiliging starten)** om dit uit te schakelen. Klik op **Voltooien**.
30. Klik met de rechtermuisknop op het pictogram ProtectTools op de werkbalk en klik op **Initialize Embedded Security restoration (Herstel geïntegreerde beveiliging initialiseren)**. Hiermee start u de wizard HP ProtectTools Embedded Security Initialization (Initialisatie geïntegreerde beveiliging).
31. Klik op **Volgende**.
32. Plaats de diskette waarop de oorspronkelijke Emergency Recovery Token-sleutel is opgeslagen in de diskettedrive. Klik op **Bladeren**, zoek de token en dubbelklik erop om de naam in het veld in te voeren. De standaardwaarde is A:\SPemRecToken.xml.
33. Typ het oorspronkelijke Token-wachtwoord en klik op **Volgende**.
34. Klik op **Bladeren**, zoek het oorspronkelijke herstelarchief en dubbelklik erop om de naam in het veld in te voeren. De standaardwaarde is C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\RecoveryArchive\SPemRecArchive.xml.
35. Klik op **Volgende**.
36. Klik op het apparaat dat u wilt herstellen en klik op **Volgende**.

37. Klik op **Volgende** om de instellingen te bevestigen.
38. Wanneer de wizard meldt dat het beveiligingsplatform is hersteld, gaat u naar stap 39.
Als de wizard meldt dat het herstellen is mislukt, gaat u terug naar stap 10. Controleer zorgvuldig de wachtwoorden, de locatie en naam van het token en de plaats en de naam van het archief.
39. Klik op **Voltooien**.
40. Als u Windows XP Professional of Home Edition gebruikt, klikt u op **Start > Alle programma's > HP ProtectTools Embedded Security Tools > User Initialization Wizard**.
Als u Windows 2000 gebruikt, klikt u op **Start > Programma's > HP ProtectTools Embedded Security Tools > User Initialization Wizard**.
41. Klik op **Volgende**.
42. Klik op **Recover your basic user key (Basisgebruikerssleutel herstellen)** en klik op **Volgende**.
43. Selecteer een gebruiker, typ het wachtwoord voor de oorspronkelijke basisgebruikerssleutel en klik op **Volgende**.
44. Klik op **Volgende** om de instellingen te bevestigen en accepteer de standaardlocatie voor de herstelgegevens.



In stap 45 tot en met 49 installeert u opnieuw de oorspronkelijke basisgebruikersconfiguratie.

45. Selecteer de gewenste beveiligingsfuncties en klik op **Volgende**.
46. Klik op de juiste e-mailclient om deze te selecteren en klik op **Volgende**.
47. Klik op het coderingscertificaat en klik op **Volgende** om dit toe te passen.
48. Klik op **Volgende** om de instellingen te bevestigen.
49. Klik op **Voltooien**.
50. Start de computer opnieuw op.



VOORZICHTIG: Ga zorgvuldig om met het basisgebruikerswachtwoord. **Zonder dit wachtwoord zijn gecodeerde gegevens niet toegankelijk en kunnen ze niet worden hersteld.**

DriveLock

DriveLock is een op industriestandaarden gebaseerde beveiligingsvoorziening die ongeoorloofde toegang tot gegevens op MultiBay vaste schijven voorkomt. DriveLock is geprogrammeerd als een uitbreiding van Computer Setup (Computerinstellingen). De voorziening is alleen beschikbaar wanneer vaste schijven worden aangetroffen die geschikt zijn voor DriveLock.

DriveLock is bedoeld voor gebruikers van HP systemen voor wie gegevensbeveiliging van het allergrootste belang is. Voor deze gebruikers zijn de kosten van de vaste schijf en het verlies van de gegevens op de schijf irrelevant vergeleken bij de schade die het gevolg kan zijn van ongeoorloofde toegang tot de inhoud van de schijf. De HP implementatie van DriveLock maakt gebruik van een beveiligingsschema met twee wachtwoorden om dit beveiligingsniveau toe te kunnen passen, maar tegelijkertijd rekening te houden met de mogelijkheid dat een wachtwoord wordt vergeten. Het ene wachtwoord wordt ingesteld en gebruikt door de systeembeheerder, het andere wordt doorgaans ingesteld en gebruikt door de eindgebruiker. Er is geen “achterdeur”: als u beide wachtwoorden vergeet, kan de schijfeenheid niet meer worden ontgrendeld. Daarom wordt u aangeraden de gegevens op de vaste schijf te kopiëren naar een bedrijfsinformatiesysteem of er regelmatig een backup van te maken.

Als u beide DriveLock wachtwoorden vergeet, kan de vaste schijf niet meer worden gebruikt. Voor gebruikers die niet beantwoorden aan het hierboven gedefinieerde profiel, is dit wellicht een onacceptabel risico. Voor gebruikers die wel beantwoorden aan dit profiel, is dit risico mogelijk acceptabel vanwege het type gegevens op de vaste schijf.

DriveLock gebruiken

De DriveLock optie staat in het menu Security (Beveiliging) van Computer Setup (Computerinstellingen). U kunt kiezen uit opties om het hoofdwachtwoord in te stellen of DriveLock in te schakelen. Om DriveLock te kunnen inschakelen, moet een gebruikerswachtwoord worden opgegeven. Aangezien de initiële configuratie van DriveLock doorgaans wordt uitgevoerd door de systeembeheerder, stelt u wellicht eerst een hoofdwachtwoord in. De systeembeheerder wordt aangeraden altijd een hoofdwachtwoord in te stellen, ongeacht of DriveLock wordt ingeschakeld. Hierdoor kan de systeembeheerder de instellingen van DriveLock wijzigen als de schijfeenheid in de toekomst wordt vergrendeld. Nadat het hoofdwachtwoord is ingesteld, kan de systeembeheerder desgewenst DriveLock inschakelen.

Als het systeem een vergrendelde vaste schijf bevat, wordt u tijdens POST gevraagd een wachtwoord in te voeren om de schijf te ontgrendelen. Als een opstartwachtwoord is ingesteld en dit overeenkomt met het gebruikerswachtwoord voor de schijf, wordt u niet gevraagd het wachtwoord nogmaals in te voeren. Als twee verschillende wachtwoorden worden gebruikt, wordt u wel gevraagd een DriveLock wachtwoord in te voeren. Gebruik hiervoor het hoofdwachtwoord of het gebruikerswachtwoord. U mag één keer een verkeerd wachtwoord invoeren. Als u twee keer een verkeerd wachtwoord invoert, wordt POST verder uitgevoerd, maar heeft u geen toegang tot de schijf.

Toepassingen van DriveLock

Het meest voorkomende gebruik van de beveiligingsvoorziening DriveLock is in een bedrijfsomgeving waarbij een systeembeheerder MultiBay vaste schijven gebruikt in bepaalde computers. De systeembeheerder is doorgaans verantwoordelijk voor het configureren van de MultiBay vaste schijven, zoals het instellen van het DriveLock hoofdwachtwoord. Als een gebruiker het gebruikerswachtwoord vergeet of de apparatuur door een andere werknemer wordt gebruikt, kan het hoofdwachtwoord worden gebruikt om het gebruikerswachtwoord opnieuw in te stellen, zodat de gegevens op de vaste schijf opnieuw toegankelijk worden.

Systeembeheerders van bedrijven die DriveLock willen gebruiken, wordt aangeraden ook een bedrijfsbeleid toe te passen voor het instellen en bijhouden van hoofdwachtwoorden, om te voorkomen dat een werknemer met opzet of per ongeluk beide DriveLock wachtwoorden wijzigt voordat hij of zij het bedrijf verlaat. In dat geval zou de vaste schijf onbruikbaar zijn en moeten worden vervangen. Als de systeembeheerder geen hoofdwachtwoord instelt, is het ook mogelijk dat de beheerder geen toegang meer heeft tot een vaste schijf en geen routinecontroles kan uitvoeren op ongeoorloofde software, andere functies voor inventarisbeheer en ondersteuning.

Als u minder strikte beveiligingsvereisten heeft, wordt u afgeraden DriveLock in te schakelen. Dit geldt bijvoorbeeld voor privégebruikers of gebruikers die doorgaans geen vertrouwelijke gegevens op hun vaste schijf hebben. Voor deze gebruikers is het mogelijke verlies van een vaste schijf wanneer beide wachtwoorden zijn vergeten, van veel groter belang dan de waarde van de gegevens die door DriveLock worden beveiligd. Gebruik het instelwachtwoord om de toegang tot Computer Setup (Computerinstellingen) en DriveLock te beperken. Door een instelwachtwoord op te geven maar dit niet aan de eindgebruiker mee te delen, kan de systeembeheerder voorkomen dat andere gebruikers DriveLock inschakelen.

Smart Cover Sensor

De Smart Cover Sensor (kapsensor) die op bepaalde modellen beschikbaar is, is een combinatie van hardware- en softwaretechnologie die u waarschuwt als de kap of het zijpaneel van de computer is verwijderd. Er zijn drie beveiligingsniveaus, zoals beschreven in onderstaande tabel:

Beveiligingsniveaus van Smart Cover Sensor

Niveau	Instelling	Beschrijving
Niveau 0	Disabled (Uitgeschakeld)	De Smart Cover Sensor is uitgeschakeld (standaardinstelling).
Niveau 1	Notify User (Gebruiker waarschuwen)	Bij het opnieuw starten van de computer verschijnt het bericht dat de kap of het zijpaneel van de computer is verwijderd.
Niveau 2	Setup Password (Instelwachtwoord)	Bij het opnieuw starten van de computer verschijnt het bericht dat de kap of het zijpaneel van de computer is verwijderd. Om door te kunnen gaan, moet het instelwachtwoord worden ingevoerd.



Deze instellingen kunnen worden gewijzigd met behulp van Computer Setup (Computerinstellingen). Raadpleeg de *Handleiding Computerinstellingen* voor meer informatie over Computer Setup.

Beveiligingsniveau van de Smart Cover Sensor instellen

U stelt het beveiligingsniveau van de Smart Cover Sensor als volgt in:

1. Zet de computer aan of start de computer opnieuw op. Klik hiervoor in Windows op **Start > Afsluiten > De computer opnieuw opstarten**.
2. Druk op **F10** zodra het monitorlampje groen gaat branden. Druk op **Enter** om een eventueel beginscherm over te slaan.



Als u niet op tijd op **F10** drukt, moet u de computer uit- en vervolgens weer inschakelen en drukt u nogmaals op **F10** om het hulpprogramma te openen.

3. Selecteer achtereenvolgens **Security (Beveiliging)** en **Smart Cover** en volg de instructies op het scherm.
4. Klik op **File (Bestand) > Save Changes and Exit (Wijzigingen opslaan en afsluiten)** voordat u het programma afsluit.

Smart Cover Lock

Het Smart Cover Lock is een softwarematige kapbeveiliging waarmee sommige HP computers zijn uitgerust. Hiermee wordt voorkomen dat onbevoegden toegang krijgen tot de interne onderdelen. Bij levering van de computer is het Smart Cover Lock niet vergrendeld.



VOORZICHTIG: U wordt aangeraden een instelwachtwoord te definiëren voor maximale beveiliging. Het instelwachtwoord voorkomt dat onbevoegden de computerconfiguratie kunnen wijzigen via Computer Setup (Computerinstellingen).



Het Smart Cover Lock is op bepaalde modellen als optie leverbaar.

Smart Cover Lock vergrendelen

U kunt het Smart Cover Lock als volgt activeren en vergrendelen:

1. Zet de computer aan of start de computer opnieuw op. Klik hiervoor in Windows op **Start > Afsluiten > De computer opnieuw opstarten**.
2. Druk op **F10** zodra het monitorlampje groen gaat branden. Druk op **Enter** om een eventueel beginscherm over te slaan.



Als u niet op tijd op **F10** drukt, moet u de computer uit- en vervolgens weer inschakelen en drukt u nogmaals op **F10** om het hulpprogramma te openen.

3. Selecteer achtereenvolgens **Security (Beveiliging)**, **Smart Cover** en de optie **Locked (Vergrendelen)**.
4. Klik op **File (Bestand) > Save Changes and Exit (Wijzigingen opslaan en afsluiten)** voordat u het programma afsluit.

Smart Cover Lock ontgrendelen

1. Zet de computer aan of start de computer opnieuw op. Klik hiervoor in Windows op **Start > Afsluiten > De computer opnieuw opstarten**.
2. Druk op **F10** zodra het monitorlampje groen gaat branden. Druk op **Enter** om een eventueel beginscherm over te slaan.



Als u niet op tijd op **F10** drukt, moet u de computer uit- en vervolgens weer inschakelen en drukt u nogmaals op **F10** om het hulpprogramma te openen.

3. Selecteer **Security (Beveiliging) > Smart Cover > Unlocked (Ontgrendelen)**.
4. Klik op **File (Bestand) > Save Changes and Exit (Wijzigingen opslaan en afsluiten)** voordat u het programma afsluit.

Smart Cover FailSafe-sleutel

Als u de Smart Cover-beveiliging heeft ingeschakeld, maar het wachtwoord niet kunt invoeren om de beveiliging uit te schakelen, heeft u een Smart Cover FailSafe-sleutel nodig om de kap van de computer te openen. U gebruikt de sleutel in de volgende situaties:

- bij een stroomonderbreking;
- bij een opstartstoring;
- bij een storing in een onderdeel van de computer (zoals de processor of de voedingseenheid);
- als u het wachtwoord vergeten bent.



VOORZICHTIG: De Smart Cover FailSafe-sleutel is bij HP verkrijgbaar. Wees voorbereid: bestel deze sleutel bij een geautoriseerde Business Partner vóórdat u er een nodig heeft.

U kunt de FailSafe-sleutel als volgt aanschaffen:

- Neem contact op met een HP Business Partner.
- Bel het telefoonnummer dat in de garantieverklaring wordt genoemd.

Raadpleeg de *Handleiding voor de hardware* voor meer informatie over de Smart Cover FailSafe-sleutel.

MBR-beveiliging

De Master Boot Record (MBR, hoofdopstartrecord) bevat informatie die nodig is om vanaf een schijf te kunnen opstarten en toegang te krijgen tot de gegevens op die schijf. Met de MBR-beveiliging kunnen onbedoelde of opzettelijke wijzigingen in de MBR worden voorkomen, zoals wijzigingen die worden veroorzaakt door bepaalde computervirussen of door onjuist gebruik van bepaalde schijfhulpprogramma's. Ook kunt u hiermee de vorige, ongewijzigde MBR herstellen als wijzigingen in de MBR worden gedetecteerd wanneer het systeem opnieuw wordt opgestart.

U schakelt MBR-beveiliging als volgt in:

1. Zet de computer aan of start de computer opnieuw op. Klik hiervoor in Windows op **Start > Afsluiten > De computer opnieuw opstarten**.
2. Druk op **F10** zodra het monitorlampje groen gaat branden. Druk op **Enter** om een eventueel beginscherm over te slaan.



Als u niet op tijd op **F10** drukt, moet u de computer uit- en vervolgens weer inschakelen en drukt u nogmaals op **F10** om het hulpprogramma te openen.

3. Selecteer **Security (Beveiliging) > Master Boot Record Security (MBR-beveiliging) > Enabled (Inschakelen)**.
4. Selecteer **Security (Beveiliging) > Save Master Boot Record (MBR opslaan)**.
5. Klik op **File (Bestand) > Save Changes and Exit (Wijzigingen opslaan en afsluiten)** voordat u het programma afsluit.

Wanneer de MBR-beveiliging is ingeschakeld, wordt via het BIOS voorkomen dat in de MS-DOS-stand of de Veilige modus van Windows wijzigingen worden aangebracht in de MBR van de huidige opstartschijf.



De meeste besturingssystemen regelen de toegang tot de MBR van de huidige opstartschijf. Het BIOS kan geen wijzigingen voorkomen die worden aangebracht terwijl het besturingssysteem actief is.

Wanneer de computer wordt ingeschakeld of opnieuw wordt opgestart, wordt de MBR van de huidige opstartschijf door het BIOS vergeleken met de laatst opgeslagen MBR. Als hierbij wijzigingen worden aangetroffen en de huidige opstartschijf dezelfde is als de schijf waarvan de MBR eerder is opgeslagen, wordt het volgende bericht weergegeven:

1999 – Master Boot Record has changed (MBR is gewijzigd).

Druk op een willekeurige toets om het hulpprogramma Computer Setup (Computerinstellingen) te starten en de MBR-beveiliging te configureren.

Nadat u het hulpprogramma heeft gestart, kiest u een van de volgende mogelijkheden:

- de MBR van de huidige opstartschijf opslaan;
- de eerder opgeslagen MBR herstellen;
- de MBR-beveiliging uitschakelen.

U moet het instelwachtwoord kennen, als dit is gedefinieerd.

Als wijzigingen worden aangetroffen terwijl de huidige opstartschijf **niet** de schijf is waarvan de MBR eerder is opgeslagen, wordt het volgende bericht weergegeven:

2000 – Master Boot Record Hard Drive has changed (Vaste schijf van MBR is gewijzigd).

Druk op een willekeurige toets om het hulpprogramma Computer Setup (Computerinstellingen) te starten en de MBR-beveiliging te configureren.

Nadat u het hulpprogramma heeft gestart, kiest u een van de volgende mogelijkheden:

- de MBR van de huidige opstartschijf opslaan;
- de MBR-beveiliging uitschakelen.

U moet het instelwachtwoord kennen, als dit is gedefinieerd.

In het onwaarschijnlijke geval dat een eerder opgeslagen MBR beschadigd is, wordt het volgende bericht weergegeven:

1998 – Master Boot Record has been lost (MBR is verloren gegaan).

Druk op een willekeurige toets om het hulpprogramma Computer Setup (Computerinstellingen) te starten en de MBR-beveiliging te configureren.

Nadat u het hulpprogramma heeft gestart, kiest u een van de volgende mogelijkheden:

- de MBR van de huidige opstartschijf opslaan;
- de MBR-beveiliging uitschakelen.

U moet het instelwachtwoord kennen, als dit is gedefinieerd.

Voordat u de huidige opstartschijf partitioneert of formatteert

Controleer of de MBR-beveiliging is uitgeschakeld voordat u de huidige opstartschijf opnieuw partitioneert of formatteert. Door sommige schijfhulpprogramma's, zoals FDISK en FORMAT, kan een update van de MBR worden uitgevoerd. Als u de schijf opnieuw partitioneert of formatteert terwijl de MBR-beveiliging is ingeschakeld, kan dit leiden tot foutberichten van het schijfhulpprogramma of tot een waarschuwing van de MBR-beveiliging wanneer u de computer weer inschakelt of opnieuw opstart. U schakelt de MBR-beveiliging als volgt uit:

1. Zet de computer aan of start de computer opnieuw op. Klik hiervoor in Windows op **Start > Afsluiten > De computer opnieuw opstarten**.
2. Druk op **F10** zodra het monitorlampje groen gaat branden. Druk op **Enter** om een eventueel beginscherm over te slaan.



Als u niet op tijd op **F10** drukt, moet u de computer uit- en vervolgens weer inschakelen en drukt u nogmaals op **F10** om het hulpprogramma te openen.

3. Selecteer **Security (Beveiliging) > Master Boot Record Security (MBR-beveiliging) > Disabled (Uitschakelen)**.
4. Klik op **File (Bestand) > Save Changes and Exit (Wijzigingen opslaan en afsluiten)** voordat u het programma afsluit.

Kabelslotvoorziening

De achterkant van de computer is voorzien van een bevestigingspunt voor een kabelslot zodat de computer fysiek aan de werkplek kan worden bevestigd.

Raadpleeg de *Handleiding voor de hardware* op de cd *Documentation Library* voor geïllustreerde instructies.

Identificatie van vingerafdrukken

Dankzij HP technologie voor de identificatie van vingerafdrukken is het niet langer nodig dat de eindgebruiker wachtwoorden invoert en wordt de netwerkbeveiliging verbeterd. Bovendien wordt het aanmelden vereenvoudigd en nemen de beheerkosten van bedrijfsnetwerken af. Aangezien deze optie gunstig geprijsd is, is deze niet uitsluitend voorbehouden aan hightech organisaties met behoefte aan strikte beveiliging.



Ondersteuning van de technologie voor de identificatie van vingerafdrukken is afhankelijk van het model.

Voor meer informatie bezoekt u:

<http://h18000.www1.hp.com/solutions/security>.

Foutberichten en fouterstel

Deze computer is uitgerust met voorzieningen voor foutberichten en fouterstel, waarbij innovatieve hardware- en softwaretechnologie voorkomt dat essentiële gegevens verloren gaan. Ook blijft ongeplande uitvaltijd van de apparatuur tot een minimum beperkt.

Wanneer zich een storing voordoet, verschijnt een lokale waarschuwing met een beschrijving van de fout en de aanbevolen acties. U kunt vervolgens de huidige systeemstatus bekijken met behulp van HP Client Manager. Als de computer is aangesloten op een netwerk dat wordt beheerd met HP Insight Manager, HP Client Manager of andere applicaties voor systeembeheer, worden de foutberichten ook naar de betreffende applicatie gestuurd.

Schijfbeveiligingssysteem

Het schijfbeveiligingssysteem DPS (Drive Protection System) is een diagnosehulpmiddel dat in de vaste schijf van bepaalde HP computers is ingebouwd. DPS is bedoeld om een diagnose te stellen van problemen met de vaste schijf, zodat de vaste schijf nietodeloos wordt vervangen.

Tijdens de productie van HP computers wordt elke geïnstalleerde vaste schijf met DPS getest en wordt de belangrijkste informatie permanent naar de schijf geschreven. Elke keer dat DPS wordt uitgevoerd, worden de testresultaten naar de vaste schijf geschreven. De geautoriseerde Business Partner gebruikt deze informatie om de omstandigheden te achterhalen die het uitvoeren van DPS noodzakelijk maakten. Raadpleeg de handleiding *Problemen oplossen* voor informatie over het gebruik van DPS.

Voedingseenheid met beveiliging tegen spanningspieken

Een geïntegreerde voedingseenheid met beveiliging tegen spanningspieken biedt grotere betrouwbaarheid bij onverwachte spanningspieken. Hierdoor kan het systeem spanningspieken tot maar liefst 2000 V weerstaan zonder dat het systeem uitvalt of er gegevens verloren gaan.

Temperatuursensor

De temperatuursensor is een hardware- en softwarematige voorziening die de interne temperatuur van de computer in de gaten houdt. Er verschijnt een waarschuwing wanneer het normale bereik wordt overschreden en u krijgt de gelegenheid om actie te ondernemen voordat interne onderdelen beschadigd raken of gegevens verloren gaan.

Index

A

- Aan/uit-knop configureren 18
- Aan/uit-knop met twee standen 18
- ActiveUpdate 6
- Afstand, ROM-flash op 7
- Altiris 4
- Altiris PC Transplant Pro 5

B

- Beperken, toegang tot computer 20
- Bestellen
 - FailSafe-sleutel 45
- Besturingssystemen, belangrijke informatie 19
- Beveiligen
 - vaste schijven 50
- Beveiliging
 - DriveLock 41 tot 42
 - MBR (Master Boot Record) 46 tot 48
 - MultiBay 41 tot 42
 - ProtectTools 31 tot 40
 - Smart Cover Sensor 43, 44 tot 45
 - wachtwoord 25
- Beveiligingsinstellingen, configureren 20
- Beveiligingsvoorzieningen, tabel 21

C

- Computer Setup (Computerinstellingen) 10
- Configureren, aan/uit-knop 18

D

- Diagnosehulpmiddel voor vaste schijven 50
- DiskOnKey
 - zie ook* HP Drive Key
 - opstarten 13 tot 18
- Drivelock 41 tot 42

E

- Eerste configuratie 2

F

- FailSafe Boot Block ROM 8
- FailSafe-sleutel
 - waarschuwing 45
- FailSafe-sleutel bestellen 45
- Formatteren, vaste schijf
 - belangrijke informatie 48
- Foutberichten 49

G

- Geïntegreerde beveiliging, ProtectTools 31 tot 40

H

- Herstellen
 - gecodeerde gegevens 36 tot 40
- Herstellen, software 2
- Herstellen, systeem 8
- HP Client Manager 4
- HP Drive Key
 - zie ook* DiskOnKey
 - opstarten 13 tot 18

I

- Installatie op afstand 3
- Installatie repliceren 10
- Installatiesoftware 2
- Instellingen
 - eerste 2
- Instelwachtwoord
 - instellen 25
 - invoeren 27
 - ProtectTools 32
- Instelwachtwoord wijzigen 28
- Instelwachtwoord wissen 29
- Interne temperatuur van computer 50
- Internetadressen, zie Websites
- Inventarisbeheer 20
- Invoeren
 - instelwachtwoord 27
 - opstartwachtwoord 27

K

- Kabelslotvoorziening 49
- Kapbeveiliging 44
 - waarschuwing 44
- Kloonsoftware 2

M

- MBR-beveiliging 46 tot 48
- Melding van wijzigingen 6
- MultiBay beveiliging 41 tot 42

N

- Nationaal toetsenbord
 - scheidingstekens 30
- Noodherstel, ProtectTools 36 tot 40

O

- Ongeldig systeem-ROM 8
- Ontgrendelen
 - Smart Cover Lock 45

- Opstartapparaat
 - diskette 12
 - DiskOnKey 13 tot 18
 - HP Drive Key 13 tot 18
 - maken 12 tot 18
 - USB-apparaat voor flashmedia 13 tot 18
- Opstartschijf
 - belangrijke informatie 48
- Opstartwachtwoord
 - invoeren 27
- Opstartwachtwoord wijzigen 28
- Opstartwachtwoord wissen 29

P

- Partitioneren, vaste schijf
 - belangrijke informatie 48
- PCN (Proactive Change Notification) 6
- Preboot Execution Environment (PXE) 3
- Proactive Change Notification (PCN) 6
- ProtectTools Embedded Security 31 tot 40
 - Emergency Recovery Key 33
 - noodherstel 36 tot 40
 - wachtwoorden
 - Basic User (Basisgebruiker) 35
 - Emergency Recovery Token 33
 - instel- 32
 - Take Ownership 33
- PXE (Preboot Execution Environment) 3

R

- Remote System Installation starten 3
- ROM
 - toetsenbordlampjes, tabel 9
- ROM beveiligen
 - waarschuwing 7
- ROM upgraden 7
- ROM, ongeldig 8
- ROM-flash op afstand 7

S

- Scheidingstekens
 - tabel 30
- Schijfeenheden beveiligen 50
- Smart Cover FailSafe-sleutel bestellen 45
- Smart Cover Lock 44
- Smart Cover Lock ontgrendelen 45
- Smart Cover Lock vergrendelen 44
- Smart Cover Sensor 43, 44 tot 45
 - beveiligingsniveaus 43
 - instellen 43
- Software
 - Computer Setup (Computerinstellingen) 10
 - Drive Protection System 50
 - FailSafe Boot Block ROM 8
 - foutberichten en foutherstel 49
 - inventarisbeheer 20
 - MBR-beveiliging 46 tot 48
 - meerdere computers updaten 6
 - Remote System Installation 3
 - ROM-flash op afstand 7
 - System Software Manager 6
- Software aanpassen 2
- Software herstellen 2
- Software integreren 2
- Spanningspieken
 - beveiliging in voedingseenheid 50
- SSM (System Software Manager) 6
- Systeemherstel 8
- System Software Manager (SSM) 6

T

- Temperatuur in computer 50
- Temperatuursensor 50
- Toegang tot computer beperken 20
- Toetsenbord

- scheidingstekens 30

- Toetsenbordlampjes,ROM 9

- Twee standen voor aan/uit-knop 18

U

- Upgraden, ROM 7
- URL's (websites). zie Websites
- USB-apparaat voor flashmedia, opstarten 13 tot 18

V

- Vaste schijf, klonen 2
- Vaste schijven
 - diagnosehulpmiddel 50
- Veranderen van besturingssysteem 19
- Vergrendelen
 - Smart Cover Lock 44
- Vingerafdrukken
 - identificatie 49
- Voedingseenheid met beveiliging tegen spanningspieken 50
- Vooraf geïnstalleerd software-image 2

W

- Waarschuwing
 - FailSafe-sleutel 45
 - kapbeveiliging 44
- Waarschuwingen
 - ROM beveiligen 7
- Wachtwoord
 - beveiliging 25
 - instel- 25
 - instellen 27
 - opstarten 27
 - ProtectTools 32 tot 35
- Wachtwoord wijzigen 28
- Wachtwoord wissen 29, 30

Websites

- ActiveUpdate 6
- Altiris PC Transplant Pro 5
- HP Client Manager 4
- HPQFlash 8
- instellingen kopiëren 12
- ondersteuning bij software 19
- PC deployment 2
- Proactive Change Notification 6
- ROM-flash 7
- ROM-flash op afstand 7

- ROMPac-images 7
- System Software Manager (SSM) 6
- technologie voor identificatie van
vingerafdrukken 49

- Altiris 5

Wijzigen

- wachtwoord 28

Wijzigingen melden 6

Wissen

- wachtwoord 29, 30